

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A method for protecting an electronic system implementing a cryptographic process involving calculation of a modular exponentiation of a quantity ( $x$ ), said modular exponentiation using a secret exponent ( $d$ ), comprising breaking down said secret exponent ( $d$ ) into a plurality of  $k$  unpredictable values ( $d_1, d_2, \dots, d_k$ ), wherein  $k$  is greater than 2, and at least one of said ( $k-1$ ) values has a length at least equal to 64 bits, the sum of which is equal to said secret exponent ( $d$ ) including:

deriving ( $k-1$ ) unpredictable values ( $d_1, d_2, \dots, d_{k-1}$ ), using a random generator;  
obtaining a final unpredictable value ( $d_k$ ) from the difference between the  
secret exponent ( $d$ ) and the ( $k-1$ ) unpredictable values ( $d_1, d_2, \dots, d_{k-1}$ ),  
creating  $k$  intermediate results by performing modular exponentiation on the  
quantity ( $x$ ) using the  $k$  unpredictable values ( $d_1, d_2, \dots, d_{k-1}, d_k$ ); and  
calculating a final result, based on the  $k$  intermediate results, equal to the  
modular exponentiation of the quantity ( $x$ ) using the secret exponent ( $d$ ).

Claims 2-4 (Cancelled)

5. (Previously Presented) Utilizing the method according to claim 1 in a smart card comprising information processing means.

6. (Previously Presented) Utilizing the method according to claim 1 for protecting a cryptographic calculation process using the RSA algorithm.

7. (Previously Presented) Utilizing the method according to claim 1 for protecting a cryptographic calculation process using the Rabin algorithm.

8. (Currently Amended) A method for protecting an electronic system implementing a cryptographic process involving calculation of a modular exponentiation of a quantity ( $x$ ), said modular exponentiation using a secret exponent ( $d$ ), comprising:

breaking down said secret exponent ( $d$ ) into a plurality of  $k$  unpredictable values ( $d_1, d_2, \dots, d_k$ ), the sum of which is equal to said secret exponent;

obtaining said unpredictable values ( $d_1, d_2, \dots, d_k$ ) by deriving ( $k-1$ ) values by means of a random generator[[;]],

wherein k is greater than 2, and at least one of said (k-1) values has a length at least equal to 64 bits, by raising the quantity ( $x$ ) by an exponent comprising a final value and obtaining a set of results for each of said  $k$  values and calculating a product of the set of results and taking the difference between the secret exponent and the ( $k-1$ ) values to derive the final value.

Claim 9 (Cancelled)

10. (Currently Amended) A smart card adapted to protect an electronic system comprising:

means for implementing a cryptographic process involving calculation of a modular exponentiation of a quantity ( $x$ ), said modular exponentiation using a secret exponent ( $d$ ), comprising breaking down said secret exponent ( $d$ ) into a plurality of  $k$  unpredictable values ( $d_1, d_2, \dots, d_k$ ), the sum of which is equal to said secret exponent, means for obtaining said unpredictable values ( $d_1, d_2, \dots, d_k$ ) by a random generator for deriving  $(k-1)$  values, wherein  $k$  is greater than 2, and at least one of said  $(k-1)$  values has a length at least equal to 64 bits, and means for taking the difference between the secret exponent and the  $(k-1)$  values to derive a final value.

11. (Previously Presented) A smart card according to claim 10, wherein calculation of the modular exponentiation is performed by:

- a) raising the quantity ( $x$ ) by an exponent comprising said value to obtain a set of results for each of said  $k$  values and
- b) calculating a product of the results obtained.